



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/500,370

07/28/2004

Jaakko Rajaniemi

59864.01048

7601

32294

7590

02/21/2008

SQUIRE, SANDERS & DEMPSEY L.L.P.

14TH FLOOR

8000 TOWERS CRESCENT

TYSONS CORNER, VA 22182

EXAMINER

HOLLIDAY, JAIME MICHELE

ART UNIT

PAPER NUMBER

2617

MAIL DATE

DELIVERY MODE

02/21/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/500,370	<b>Applicant(s)</b> RAJANIEMI, JAAKKO	
	<b>Examiner</b> Jaime M. Holliday	<b>Art Unit</b> 2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 08 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) 22-26 and 28 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-21, 27 and 29-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Response to Arguments***

1. Applicant's arguments with respect to claims 1-21, 27 and 29-37 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
3. **Claims 1-6-14, 16-21, 27, 29-34, 36 and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chavez et al. (U.S. Patent # 6,591,102 B1)** in view of **Wright (U.S. Patent # 6,957,061 B1)**, and in further view of **Henry et al. (US 6,856,800 B1)**.

Consider **claim 1**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, reading on the claimed "method for providing access to a service for a user in a communication system," (col. 1 line 67- col. 2 lines 2), comprising: receiving an outgoing service request from a mobile handset, reading on the claimed "user," and a base station reading a memory for storing authentication information for mobile handsets services by the base station, reading on the claimed "node." The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the

base station transmits a request for authentication information to the mobile switching system, wherein the mobile switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives, reading on the claimed "using a specific record, associated with said user, at a node in the communication system, determines that a user characteristic is to be verified prior to providing access to said service," (col. 1 lines 45-48, col. 5 lines 35-50).

However, Chavez et al. fail to specifically disclose that a specific record contains information that is used to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, reading on the claimed "method for providing access to a service for a user in a communication system," (col. 1 lines 25-30). The request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The user equipment can allow the authentication vector to be used for a predetermined time period, number of calls

or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "using a specific record, containing information which, determines that a user characteristic is to be verified with a home network prior to providing access to said service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP **202** includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home AAA server **204**. The Revoked Certificate Database contains security certificates that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The

current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access. Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "method for providing access to a service for a user in a communication system, comprising using a specific record associated with said user, wherein the specific record is stored at a server node," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 2**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 1 above**, and in addition, Henry et al. further discloses that the AP should have the public key of the mobile host's home AAA server, in the business partner database. This is set up between the access network and the mobile host's home network via a business agreement, reading on the claimed

"transferring said information from the AAA-H to the serving node in the signaling path for the service setup and/or service event and/or registration," (col. 4 lines 5-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point with information previously received from the home AAA server as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 3**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 1 above**, and in addition, Wright further discloses that before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "deciding based on said information that the authentication and/or authorization needs be verified," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

Consider **claim 4**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 1 above**, and in addition, Chavez et al. further discloses that the base station determines whether the authentication information is stored in the memory, and if it is, the base station reads the authentication information and performs normal authentication, reading on the claimed "performing the authentication and/or authorization," (col. 5 lines 25-60).

Consider **claim 5**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 4 above**, and in addition, Henry et al. further discloses that if the authentication credential is validated, the access point grants the network access device conditional access to the network, contacts the remote authentication server to verify a status of the authentication credential for the network access device; and suspends network access for the network access device in response to a message received from the remote authentication server that the authentication credential for the network access device has been revoked, reading on the claimed "performing the authentication and/or authorization by using the AAA-H," (fig. 2, col. 2 lines 18-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point and at a home AAA server as taught by Henry et al. in the method



of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 6**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 4 above**, and in addition, Chavez et al. further discloses that the base station determines whether the authentication information is stored in the memory, and if it is, the base station reads the authentication information and performs normal authentication, reading on the claimed "performing the authentication and/or authorization in the node if the required parameters are available," (col. 5 lines 25-60).

Consider **claim 7**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, reading on the claimed "method for providing a user of user equipment with access to a service from a service provider node in a wireless communication system," (col. 1 line 67- col. 2 lines 2), comprising: receiving an outgoing service request from a mobile handset, reading on the claimed "user," and a base station reading a memory for storing authentication information for mobile handsets services by the base station, reading on the claimed "node." The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the base station transmits a request for authentication information to the mobile switching system, wherein the mobile

switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives, reading on the claimed "using a user specific record, determines that a user characteristic is to be verified prior to providing access to said service; and providing access to said service responsive to said user specific record," (col. 1 lines 45-48, col. 5 lines 35-50).

However, Chavez et al. fail to specifically disclose that a specific record indicates a condition that is used to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, reading on the claimed "method for providing a user of user equipment with access to a service from a service provider node in a wireless communication system," (col. 1 lines 25-30). The request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call

duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "using a user specific record indicating a condition which, if satisfied, determines that a user characteristic is to be verified prior to providing access to said service; and providing access to said service responsive to said user specific record," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP **202** includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home AAA server **204**. The Revoked Certificate Database contains security certificates that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a

CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access. Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "method for providing a user of user equipment with access to a service, comprising using a user specific record, wherein the user specific record is stored at a server node," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 8**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose that the base station determines if the received request is for an incoming or outgoing service request. If it is for an incoming service request, the base station reads

authentication information from the incoming request. The authentication information may then be stored in a memory in base station and normal authentication is performed, reading on the claimed "determining if said condition is satisfied; and providing access to said service without verifying said user characteristic if said condition is not satisfied," (col. 5 lines 10-32).

Consider **claim 9**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose that the base station determines if the received request is for an incoming or outgoing service request. If it is for an outgoing service request, the base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the base station transmits a request for authentication information to the mobile switching system, wherein the mobile switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives, reading on the claimed "determining if said condition is satisfied; verifying said user characteristic if said condition is satisfied; and subsequent to said step of verifying the user characteristic providing access to said service if said user characteristic indicates the user is permitted access to said service," (col. 1 lines 45-48, col. 5 lines 35-50).

Consider **claim 10**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose that if the request is an incoming service request, which could be an outgoing service request including a telephone number requesting a call, the base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information, reading on the claimed "determining if said condition is satisfied when a call session between said user and said service provider node is initiated," (col. 5 lines 10-60).

Consider **claim 11**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose that if the request is an incoming service request, wherein this request could be an incoming service request from the MSC to provide a communication service to mobile handset, the base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, reading on the claimed "determining from the user specific record associated with said user if said condition exists during a call session between said user equipment and said service provider node," (col. 5 lines 25-60).

Consider **claim 12**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose receiving an outgoing service request from a mobile handset, and a base station reading a memory for storing authentication information for mobile handsets services by the base station. The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication, reading on the claimed "indicating, via said user specific record, when access to said service is permitted without determining, from data stored at a node in said home network, if access is permitted," (col. 5 lines 35-50).

However, Chavez et al. fail to specifically disclose that there are two distinct networks (home and serving) in the communication system.

Wright further discloses authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, wherein the request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed, reading on the claimed "wireless communication system comprises a serving network in which said user equipment is located, and a home network, " (col. 1 lines 25-43).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user in a serving network

that is subscribed to a home network as taught by Wright in the method of Chavez et al., in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Consider **claim 13**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose receiving an outgoing service request from a mobile handset, and a base station reading a memory for storing authentication information for mobile handsets services by the base station. The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication, reading on the claimed "storing said user specific record at a node of said serving network," (col. 5 lines 35-50).

However, Chavez et al. fail to specifically disclose that there are two distinct networks (home and serving) in the communication system.

Wright further discloses authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, wherein the request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed, reading on the claimed "wireless communication system comprises a serving network in which said user equipment is located, and a home network, " (col. 1 lines 25-43).



Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user in a serving network that is subscribed to a home network as taught by Wright in the method of Chavez et al., in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Consider **claim 14**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose that if a the service information is not stored in memory from a previous request for the service information, a request is sent to the service provider which has a database that stores all the services a mobile is allowed to receive, (col. 6 lines 20-35, col. 1 lines 35-60); the service provider then transmits the service information back to the MSC the MSC stores the information in memory, (col. 6 lines 20-65); service information is transmitted to the MSC which the information to the base station and then authentication takes place, (col. 6 lines 20-65, col. 5 lines 25-60); and if the authentication is successful service is provided to the user, reading on the claimed "generating a register message at said user equipment and transmitting said register message to a local server node of said communication system; determining if a condition indicated by said user specific record stored at said local server node is satisfied; generating an access message at said local server node indicating that access to said service is

permitted; and transmitting said access message to said service provider node,"  
(col. 6 lines 25-60).

Consider **claim 16**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Chavez et al. further disclose that if a the service information is not stored in memory from a previous request for the service information, a request is sent to the service provider which has a database that stores all the services a mobile is allowed to receive, (col. 6 lines 20-35, col. 1 lines 35-60); the service provider then transmits the service information back to the MSC the MSC stores the information in memory, (col. 6 lines 20-65); service information is transmitted to the MSC which transmits the information to the base station and then authentication takes place, (col. 6 lines 20-65, col. 5 lines 25-60); and if the authentication is successful service is provided to the user, reading on the claimed "generating an invite message at said user equipment and transmitting said invite message to a local server node of said communication system; determining if a condition indicated by said user specific record stored at said local server node is satisfied; generating an access message at said local server node indicating that access to said service is permitted; and transmitting said access message to said service provider node," (col. 5 lines 25-60).

Consider **claim 17**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as**

**applied to claim 7 above**, and in addition, Wright further discloses that before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "user characteristic comprises whether said user is authorized to access said service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to verify that a user has been authenticated as taught by Wright in the method of Chavez et al., in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Consider **claim 18**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Wright further discloses that before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "user characteristic comprises whether said user is authenticated to access said service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to verify that a user has been

authenticated as taught by Wright in the method of Chavez et al., in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Consider **claim 19**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Wright further discloses that the user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "condition determines the frequency at which said user is to be authorized and/or authenticated during a call session between said user equipment and said service provider node," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated depending on a predetermined set time as taught by Wright in the method of Chavez et al., in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Consider **claim 20**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 1 above**, and in addition, Chavez et al. further discloses that if

the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, reading on the claimed "using a specific record comprises storing a user specific record," (col. 5 lines 25-60).

Consider **claim 21**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, reading on the claimed "server node of a communication system," (col. 1 line 67- col. 2 lines 2), comprising: receiving an outgoing service request from a mobile handset, and a base station reading a memory for storing authentication information for mobile handsets services by the base station, reading on the claimed "means for receiving a message from a user equipment." The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the base station transmits a request for authentication information to the mobile switching system, wherein the mobile switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives. If the authentication is successful service is provided to the user, reading on the claimed "means for using a user specific record, associated with said user, determines that a user characteristic is to be verified prior to providing a user with access to said a service; and means for generating,

in response to said user specific record, an access message for providing said user with access to said service, thereby providing the user of the user equipment with access to a service from a service provider node," (col. 1 lines 45-48, col. 5 lines 25-60).

However, Chavez et al. fail to specifically disclose that a specific record contains information that is used to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed. The request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the

claimed "means for using a user specific record, associated with said user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing a user with access to said a service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP **202** includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home AAA server **204**. The Revoked Certificate Database contains security certificates that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP

should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access. Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "server node comprising means for storing a user specific record, associated with said user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing a user with access to a service," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 27**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, comprising: receiving an outgoing service request from a mobile handset, reading on the claimed "user equipment," and a base station reading a memory for storing authentication information for mobile handsets services by the base station. The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the



base station transmits a request for authentication information to the mobile switching system, wherein the mobile switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives. If the authentication is successful service is provided to the user, reading on the claimed "means for using a specific record associated with a user, determines that a user characteristic is to be verified prior to providing access to said service, thereby providing the user with access to the service from a service provider node," (col. 1 lines 45-48, col. 1 line 67- col. 2 lines 2, col. 5 lines 35-60).

However, Chavez et al. fail to specifically disclose that the mobile handset uses a specific record that contains information to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, (col. 1 lines 25-30). The request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The user equipment can allow the authentication vector to be

used for a predetermined time period, number of calls or total call duration.

Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "Mobile user equipment, comprising means for using a user specific record associated with a user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing said user with access to a service; and means for generating, in response to said user specific record, an access message for providing said user with access to said service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP 202 includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home

AAA server **204**. The Revoked Certificate Database contains security certificates that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access. Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "Mobile user equipment, comprising means for using a user specific record associated with a user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing said user with access to a service, wherein the user specific record is stored at a server node," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 29**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, reading on the claimed "method for providing access to a service for a user in a communication system," (col. 1 line 67- col. 2 lines 2), comprising: receiving an outgoing service request from a mobile handset, reading on the claimed "user," and a base station reading a memory for storing authentication information for mobile handsets services by the base station, reading on the claimed "serving node." The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the base station transmits a request for authentication information to the mobile switching system, wherein the mobile switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives, reading on the claimed "storing an authorization and authentication profile, associated with said user, at a serving node in a serving network; using said authorization and authentication profile at said serving node in the communication system; wherein said authorization and authentication profile, determines that a user characteristic is to be verified prior to providing access to said service," (col. 1 lines 45-48, col. 5 lines 35-50).

However, Chavez et al. fail to specifically disclose that a specific record contains information that is used to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, reading on the claimed "method for providing access to a service for a user in a communication system," (col. 1 lines 25-30). The request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "authorization and authentication profile contains information indicating a condition which if satisfied, determines that a user

characteristic is to be verified with a home network prior to providing access to said service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP **202** includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home AAA server **204**. The Revoked Certificate Database contains security certificates that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access.

Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "storing an authorization and authentication profile, associated with said user, wherein the authorization and authentication profile is stored at a serving node in a serving network," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 30**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, reading on the claimed "server node of a communication system," (col. 1 line 67- col. 2 lines 2), comprising: receiving an outgoing service request from a mobile handset, and a base station reading a memory for storing authentication information for mobile handsets services by the base station, reading on the claimed "interface for receiving a message from said user equipment." The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn't, the base station transmits a request for authentication information to the mobile switching system, wherein the mobile

switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives. If the authentication is successful, service is provided to the user, reading on the claimed "server node configured to use a user specific record, associated with said user, determines that a user characteristic is to be verified prior to providing said user with access to said a service; and generate, in response to said user specific record, an access message for providing said user with access to said service, thereby providing the user of user equipment with access to the service from a service provider node.," (col. 1 lines 45-48, col. 5 lines 25-60).

However, Chavez et al. fail to specifically disclose that a specific record contains information that is used to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed. The request for service is passed from the serving network to a home operator network to which the user equipment is directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The



user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "use a user specific record, associated with said user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing said user with access to said a service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP **202** includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home AAA server **204**. The Revoked Certificate Database contains security certificates

that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access. Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "a server node wherein the user specific record is stored in the server node," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 31**, Chavez et al. clearly show and disclose a method for transmitting feature and authentication information for wireless communication services, comprising: receiving an outgoing service request from a mobile handset, reading on the claimed "mobile user equipment comprising processor

and control means,” and a base station reading a memory for storing authentication information for mobile handsets services by the base station. The base station determines whether the authentication information is stored in the memory. If it is, the base station reads the authentication information and performs normal authentication. If it isn’t, the base station transmits a request for authentication information to the mobile switching system, wherein the mobile switching system forwards the request to a service provider wireless server. The service provider wireless server maintains records as to which services the mobile handset receives. If the authentication is successful service is provided to the user, reading on the claimed “use a user specific record associated with said user, determines that a user characteristic is to be verified prior to providing said user with access to said a service; thereby providing the user with access to the service from a service provider node,” (col. 1 lines 45-48, col. 1 line 67- col. 2 lines 2, col. 5 lines 35-60).

However, Chavez et al. fail to specifically disclose that the mobile handset uses a specific record that contains information to determine that a user is to be verified with a home network.

In the same field of endeavor, Wright clearly shows and discloses a method of authenticating mobile user equipment in a mobile telecommunications, wherein service is requested from a serving network from a user equipment not directly subscribed, (col. 1 lines 25-30). The request for service is passed from the serving network to a home operator network to which the user equipment is

directly subscribed. An authentication vector is generated in the home network, passed to the serving network, and at least part of the vector (authentication element) passed to the user equipment. The user equipment generates a predetermined key set identifier (KSI), and passes it to the serving network, (col. 1 lines 25-43). The user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made, reading on the claimed "Mobile user equipment, comprising processor and a control unit, wherein the control unit is configured to use a user specific record associated with said user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing said user with access to said a service; and generate, in response to said user specific record, an access message for providing said user with access to said service," (col. 3 lines 56-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated as taught by Wright in the method of Chavez et al., in order to reduce the amount of data transmitted from a handset to a base station (Chavez et al.; abstract).

However, Chavez et al., as modified by Wright, fail to specifically disclose that the specific record is stored at a server node.

In the same field of endeavor, Henry et al. clearly show and disclose a foreign AP **202** includes or is otherwise associated with a Business Partner Database, Revoked Certificate Database, and an Access Control Database. The Business Partner Database contains the public keys for the mobile host's home AAA server **204**. The Revoked Certificate Database contains security certificates that have been revoked before expiration. The Access Control Database stores session keys for the mobile host(s). The foreign AP has memory **222** including a CURRENT\_PUBLIC\_KEY register and a NEXT\_PUBLIC\_KEY register. The current public key of the home AAA server is stored in the CURRENT\_PUBLIC\_KEY register. After receiving the security certificate, the AP checks the signature and expiration time of the security certificate. The AP should have the public key of the mobile host's home AAA server. If the AP determines that the security certificate is invalid, the AP denies the access. Otherwise the AP checks the revoked certificate database, to determine whether the security certificate has been revoked before it was set to expire. If the certificate has been revoked, the AP denies the access request. Otherwise, the AP immediately grants temporary access to the mobile host, reading on the claimed "wherein the user specific record is stored in the server node," (col.3 lines 40-52, col. 4 lines 3-21).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point as taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 32**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 30 above**, and in addition, Chavez et al. further discloses that if the service information is not sorted in the memory the MSC requests the information from the service provider, reading on the claimed "a transmitter configured to transmit said access message to a service provider," (col. 6 lines 20-50).

Consider **claim 33**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 30 above**, and in addition, Henry et al. further discloses that the AP should have the public key of the mobile host's home AAA server, in the business partner database. This is set up between the access network and the mobile host's home network via a business agreement, reading on the claimed ""a receiver configured to receive data comprising said user specific record transmitted from a home AAA server node," (col. 4 lines 5-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to validate a users credentials locally at an access point with information previously received from the home AAA server as

taught by Henry et al. in the method of Chavez et al., as modified by Wright, in order to provide fast authentication of a mobile host (Henry et al.).

Consider **claim 34**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 30 above**, and in addition, Chavez et al. further discloses that if the service information is not sorted in the memory the MSC requests the information from the service provider, reading on the claimed "serving or proxy-call session control function node," (col. 6 lines 20-50).

Consider **claim 36**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 30 above**, and in addition, Chavez et al. further discloses that if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, reading on the claimed "a storage unit configured to store a user specific record;" (col. 5 lines 25-60).

Consider **claim 37**, the combination of Chavez et al. and Wright, as modified by Henry et al., clearly shows and discloses the claimed invention **as applied to claim 31 above**, and in addition, Chavez et al. further discloses that if the request is an incoming service request, base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed,

reading on the claimed "a storage unit configured to store a user specific record,"  
(col. 5 lines 25-60).

4. **Claims 15 and 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chavez et al. (U.S. Patent # 6,591,102 B1)** in view of **Wright (U.S. Patent # 6,957,061 B1)**, and in further view of **Basilier et al. (U.S. Patent # 6,728,536)**.

Consider **claim 15**, and **as applied to claim 14 above**, Chavez et al., as modified by Wright, clearly show and disclose the claimed invention, except that the information is specifically requested prior to storing the specific record and is transferred from the AAA-H in response.

In the same field of endeavor, Basilier et al. clearly show and disclose a method in which specific information, which may be access specific and/or application specific information is transmitted between visiting and home networks, (col. 1 line s66- col. 2 line 2). A user wished to use the mobile terminal in the visited network, and registers in the visited network. The ACS/VLR assembles a registration and/or authentication message, and sends it to the AAA-F. The AAA-F uses a NAI to locate the appropriate AAA-H, and route the message to the appropriate HLR. The HLR validates or denies the registration request, and generates an appropriate response message, which is transmitted to the visited network, reading on the claimed "prior to said storing said user specific record, generating a request message at said local server node and transmitting said request message to the home AAA server of the user; and



transferring data comprising said user specific record from said home AAA server to said local server node responsive to said request message," (fig.2 b., col. 4 line 52- col. 5 line 25, col. 6 lines 15-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user by communicating with the home network (HLR, AAA-H) as taught by Basilier et al. in the method of Chavez et al., as modified by Wright, in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Consider **claim 35**, and **as applied to claim 30 above**, Chavez et al., as modified by Wright, clearly show and disclose the claimed invention, except that the information included in the specific record specifically includes a first field for identifying the user and a second field to identify when to authenticate at the AAA-H.

In the same field of endeavor, Basilier et al. clearly show and disclose a method in which specific information, which may be access specific and/or application specific information is transmitted between visiting and home networks, (col. 1 line s66- col. 2 line 2). A user wished to use the mobile terminal in the visited network, and registers in the visited network. The ACS/VLR assembles a registration and/or authentication message, and sends it to the AAA-F. The AAA-F uses a NAI, or the significant digits of the IMSI, to locate the appropriate AAA-H, and route the message to the appropriate HLR. The HLR validates or denies the registration request, and generates an appropriate

response message, which is transmitted to the visited network, reading on the claimed "user specific record comprises a first data field identifying said user and a second data field determining when authentication and/or authorization of said user is required in order to access said service," (fig.2 b., col. 4 line 52- col. 5 line 25, col. 6 lines 15-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user by communicating with the home network (HLR, AAA-H) as taught by Basilier et al. in the method of Chavez et al., as modified by Wright, in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

### ***Conclusion***

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

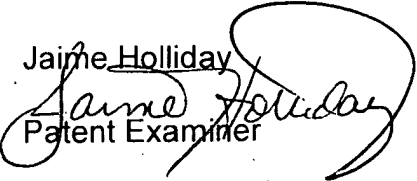
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaime M. Holliday whose telephone number is (571) 272-8618. The examiner can normally be reached on Monday through Friday 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Feild can be reached on (571) 272-4090. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jaime Holliday  
  
Patent Examiner

  
CHARLES N. APPIAH  
SUPERVISORY PATENT EXAMINER